University of Wisconsin-Madison
Policy and Procedure

Policy Number:	8.8
Policy Title:	Notification and Reporting in the Case of Breach of Unsecured Protected Health Information
Effective Date:	September 30, 2014
Last Revision Date:	September 30, 2014
Page 1 of 12	

I. Policy

The Health Information Technology for Economic and Clinical Health Act ("HITECH") regulations contain requirements for notifying individuals in the event of a breach of their unsecured protected health information. In addition, HITECH contains requirements for notifying the Office of Civil Rights ("OCR") regarding breaches. UW-Madison investigates potential breaches of protected health information (hereafter "incidents") and determines if there is a breach, according to HITECH regulations. If there is a breach, UW-Madison makes notification to the patients whose health information is involved and makes the report to OCR as required by HITECH.

II. Definitions

A. Discovery: The first day on which an incident is known to UW-Madison (including by any person, other than the individual committing the breach, that is an employee, officer, or other agent of UW-Madison) or should reasonably have been known to UW-Madison to have occurred.

B. Breach: The acquisition, access, use, or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the protected health information.

Breach excludes:

1. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.

2. Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health

information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.

3. A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

C. Disclosure**:** The release, transfer, provision of access to, or divulging in any manner of PHI by an individual within the HCC or ACE (see definitions below) with a person or entity outside the HCC or ACE.

D. HITECH: The Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to promote the adoption and meaningful use of health information technology.

E. Protected Health Information ("PHI"): Health information or health care payment information, including demographic information collected from an individual, which identifies the individual or can be used to identify the individual. PHI does not include student records held by educational institutions or employment records held by employers.

F. University of Wisconsin Affiliated Covered Entity ("UW ACE"): The UW-Madison Health Care Component (except University Health Services and the State Laboratory of Hygiene), the University of Wisconsin Medical Foundation and the University of Wisconsin Hospital and Clinics. See Privacy Policy # 1.2 "Designation of UW Affiliated Covered Entity".

G. University of Wisconsin-Madison Health Care Component ("UW HCC"): Those units of the University of Wisconsin-Madison that have been designated by the University as part of its health care component under

HIPAA. See Privacy Policy # 1.1 "Designation of UW-Madison Health Care Component" for a listing of these units.

H. Unsecured PHI: PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Department of Health and Human Services.

III. Procedures

A. Investigations of incidents (Paper or Oral Only)

1. Anyone who becomes aware of an incident involving paper records or oral statements only must call the UW-Madison HIPAA Privacy Officer within 24 hours of the discovery of the potential or actual breach of PHI. This may be followed up by email. Contact information for the HIPAA Privacy Officer can be found at hipaa.wisc.edu.

2. Examples of incidents involving paper records or oral statements only include:

- Patient is handed a copy of the wrong after visit summary;
- A paper copy of a portion of a patient's medical record is removed from the covered entity by a health care provider;
- A health care provider is overheard discussing patient's medical information in the elevator or cafeteria.
- An abstract or poster for presentation at an event or conference that contains PHI without appropriate authorization.

4. The HIPAA Privacy Officer, or the HIPAA Privacy and Security Program Coordinator at the direction of the HIPAA Privacy Officer, shall notify the HIPAA Privacy Coordinator of the applicable HCC unit within 24 hours of being notified of the potential or actual breach.

5. The HIPAA Privacy Officer shall lead the investigation and, in coordination with the Coordinator of the applicable HCC unit or his/her designee, shall complete the UW-Madison HIPAA Breach Analysis Form within 14 calendar days, absent exigent circumstances. The Privacy Officer shall notify the HIPAA Privacy and Security Operations Committee if an investigation must continue beyond 14 calendar days and the reason for the delay.

6. The HIPAA Privacy and Security Program Coordinator shall log the incident into the Incident/Breach Tracking Form, and shall update the Tracking Form with information from the HIPAA Breach Analysis Form and with information about notices sent to affected individuals and the Department of Health and Human Services.

7. The HIPAA Privacy and Security Program Coordinator shall forward the completed HIPAA Breach Analysis Form to the UW-Madison HIPAA Privacy and Security Operations Committee.

B. All Other Investigations of Incidents.

1. Anyone who becomes aware of an incident not described in III.A. above must contact the following:

   a. Either their local/departmental IT office or the DoIT Help Desk immediately at 608-264-HELP (4357); **and**

   b. The HIPAA Privacy Officer immediately. Contact information for the HIPAA Privacy Officer can be found at hipaa.wisc.edu.

2. The local/departmental IT office shall immediately notify the DoIT Help Desk, or vice versa, upon being notified of a potential or actual breach per III.B.1. above.

3. The HIPAA Privacy Officer shall immediately notify the HIPAA Security Officer upon being notified of a potential or actual breach per III.B.1. above. If the HIPAA Security Officer becomes aware of an Incident, s/he shall notify the HIPAA Privacy Officer and the local/departmental IT office.

4. If the HIPAA Privacy Officer, in consultation with the HIPAA Security Officer as needed, determines that additional information is not needed from an investigation through the UW-Madison Chief Information Office (as described below in III.B.5.) to determine whether a breach has occurred, the investigation shall proceed as outlined in III.A.4.-7. above.

5. If additional information from a CIO investigation is needed to determine whether a breach occurred, or as otherwise directed by the HIPAA Security Officer, the CIO's Information Security Officer shall conduct an investigation and provide his/her findings to the HIPAA Privacy and Security Officers without unreasonable delay and in no case more than 30 days from the date of discovery of the incident.

6. Upon receipt of the Information Security Officer's report, the investigation shall proceed as outlined in III.A.5.-7. above.

7. If the HIPAA Security Officer determines that an Administrative Leadership Team ("ALT") should be assembled as described in the CIO's Information Incident Reporting and Response Policy, the ALT shall include the HIPAA Privacy Officer.

8. Upon completion of its analysis, the ALT shall forward a copy of its determinations to the HIPAA Privacy and Security Operations Committee.

C. Breach Determination

1. The final determination whether a breach per the HITECH regulations has occurred will be made by the HIPAA Privacy Officer in consultation with the UW-Madison HIPAA Privacy and Security Operations Committee, as time permits or as otherwise is needed.

2. In determining whether a breach occurred which requires notification to patients and reporting to OCR, the HIPAA Privacy Officer shall consider the following: an impermissible use or disclosure is presumed to be a breach unless it can be demonstrated that there is a low probability that the PHI has been compromised based on the following:

   a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.

   b. The unauthorized person who used the PHI or to whom the disclosure was made.

   c. Whether the PHI was actually acquired or viewed.

   d. The extent to which the risk to the PHI has been mitigated.

   e. Other relevant factors may be considered when necessary.

3. The HIPAA Privacy Officer, on behalf of the HIPAA Privacy and Security Operations Committee, will notify the UW-Madison HIPAA Privacy and Security Executive Board of any required breach notifications.

D. Breach Notifications. If it is determined that a breach of unsecured PHI has occurred, the following notifications are made:

1. Notification to Affected Individuals.

a. Without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, the HIPAA Privacy Officer notifies each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of a breach.

b. The HIPAA Privacy Officer shall draft and sign the notification letter, in consultation as needed with the Privacy Coordinator of the relevant HCC unit in the drafting. The HIPAA Privacy and Security Program Coordinator shall ensure timely mailing of the notification letters.

c. The notification, written in plain language, shall include to the extent possible:

i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

ii. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

iii. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

iv. A brief description of what UW-Madison is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

v. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

d. The notification required shall be provided in the following form:

i. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

ii. If UW-Madison knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

e. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice reasonably calculated to reach the individual shall be provided (this does not apply to the next of kin or personal representative of the individual).

i. In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be

provided by an alternative form of written notice, telephone, or other means.

ii. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

(a) Be in the form of either a conspicuous posting for a period of 90 days on the hippa.wisc.edu home page of, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

(b) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured PHI may be included in the breach.

f. In any case deemed to require urgency because of possible imminent misuse of unsecured PHI, the HIPAA Privacy Officer may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided as described above.

2. Notification to the Secretary of US Department of Health and Human Services (HSS).

a. For breaches of unsecured PHI involving 500 or more individuals, the HIPAA Privacy Officer provides notification to the Secretary contemporaneously with the notice to affected individuals in the manner specified on the HHS Web site.

b. For breaches of unsecured PHI involving less than 500 individuals, the HIPAA Privacy Officer or the Privacy and Security Program Coordinator at his/her direction, maintains a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provides the notification for breaches discovered during the preceding calendar year, in the manner specified on the HHS web site.

3. Notification to the Media. For a breach of unsecured PHI involving more than 500 residents of the State, the UW-Madison HIPAA Privacy Officer in conjunction with University Communications and Marketing shall, following the discovery of the breach, notify prominent media outlets serving the State.

4. Law Enforcement Delay. If a law enforcement official states that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, the HIPAA Privacy Officer shall:

   a. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

   b. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

5. The HIPAA Privacy Officer will notify the HIPAA Privacy and Security Operations Committee when all required notifications have been made.

E. In the event an incident involves research subjects, the HIPAA Privacy Officer shall notify the appropriate Intuitional Review Board ("IRB") upon learning of the incident if unclear that the IRB is already aware, and shall work with such IRB to ensure that any proposed remediation does not conflict with IRB determinations, policies or laws governing human subjects research.

F. Breaches and incidents determined not to be breaches will be reported to the HIPAA Privacy and Security Operations Committee by the HIPAA Privacy Officer for discussion of possible remedial actions.

IV. Documentation Requirements

The UW-Madison HIPAA Breach Analysis Form must be completed for each breach investigation.

V. Forms

UW-Madison HIPAA Breach Analysis Form
Incident/Breach Tracking Form

VI. References

45 CFR Subpart D

VII. Related Policies

None

VIII. For Further Information

For further information concerning this policy, please contact the UW-Madison HIPAA Privacy Officer or the appropriate unit HIPAA Privacy Coordinator or sub-Coordinator. Contact information is available within the "Contact Us" tab at hipaa.wisc.edu.

Reviewed By
UW-Madison HIPAA Privacy Officer
UW-Madison Office of Legal Affairs

Approved By
Interim HIPAA Privacy and Security Operations Committee